m-Sequences of Different Lengths with Four-Valued Cross Correlation

Tor Helleseth and Alexander Kholosha and Aina Johanssen
The Selmer Center,
Department of Informatics, University of Bergen
PB 7800
N-5020 Bergen, Norway

February 2, 2008

Abstract. Considered is the distribution of the cross correlation between m-sequences of length $2^m - 1$, where m is even, and m-sequences of shorter length $2^{m/2} - 1$. The infinite family of pairs of m-sequences with four-valued cross correlation is constructed and the complete correlation distribution of this family is determined.

Keywords: m-sequences, cross correlation, linearized polynomials.

1 Introduction

Let $\{a_t\}$ and $\{b_t\}$ be two binary sequences of length p. The cross-correlation function between these two sequences at shift τ, where $0 \leq \tau < p$, is defined by

$$C(\tau) = \sum_{t=0}^{p-1} (-1)^{a_t + b_{t+\tau}} \quad .$$

A well studied problem is to find the cross-correlation function between two binary m-sequences $\{s_t\}$ and $\{s_{dt}\}$ of the same length $2^m - 1$ that differ by a decimation d such that $\gcd(d, 2^m - 1) = 1$. An overview of known results can be found in Helleseth [1], Helleseth and Kumar [2] and Dobbertin et. al. [3].

Recently, Ness and Helleseth [4] studied the cross correlation between any m-sequence $\{s_t\}$ of length $p = 2^m - 1$ and any m-sequences $\{u_{dt}\}$ of shorter length $2^{m/2} - 1$, where m is even and $\gcd(d, 2^{m/2} - 1) = 1$. For convenience, $\{u_t\}$ is selected to be the m-sequence used in the small Kasami sequence family. The only known families of m-sequences of these periods giving a two-valued cross correlation are related to the Kasami sequences [5] and are obtained taking $d = 1$. Further, families with three-valued cross correlation have been constructed by Ness and Helleseth in [4] and [6]. These results were generalized by Helleseth, Kholosha and Ness [7] who covered all known cases of three-valued cross correlation and conjectured that these were the only existing.

In this paper, we consider pairs of sequences with a four-valued cross correlation. The first family with such a property was described in [8]. We completed a full search for all values of $m \leq 32$ and revealed a few examples that did not fit into the known family. Most of the cases with four-valued cross correlation occur for $m = 2nk$ with $n > 2$ odd and the decimation

$$d = \frac{2^{nk} + 1}{2^k + 1} \quad \text{with} \quad k > 1 \ .$$

The main result of this paper is finding the distribution for this four-valued cross correlation. Note that the family found in [8] corresponds to the latter decimation when setting $n = 3$.

In Section 2, we present preliminaries needed to prove our main results. In Section 3, we give the distribution of the number of zeros of a particular affine polynomial $A_a(x)$. Section 4 provides the distribution of the number of zeros of a special linearized polynomial $L_a(z)$. The zeros of these two polynomials are useful when obtaining the cross-correlation values. Section 5 determines the cross-correlation distribution of our four-valued family.

2 Preliminaries

Let $\mathrm{GF}(q)$ denote a finite field with q elements and let $\mathrm{GF}(q)^* = \mathrm{GF}(q) \setminus \{0\}$. The finite field $\mathrm{GF}(q^l)$ is a subfield of $\mathrm{GF}(q^m)$ if and only if l divides m. The trace mapping from $\mathrm{GF}(q^m)$ to the subfield $\mathrm{GF}(q^l)$ is defined by

$$\mathrm{Tr}_l^m(x) = \sum_{i=0}^{m/l-1} x^{q^{li}} \ .$$

In the case when $l = 1$, we use the notation $\mathrm{Tr}_m(x)$ instead of $\mathrm{Tr}_1^m(x)$. The norm $\mathrm{N}_l^m(x)$ of $x \in \mathrm{GF}(q^m)$ over the subfield $\mathrm{GF}(q^l)$ is defined by

$$\mathrm{N}_l^m(x) = \prod_{i=0}^{m/l-1} x^{q^{li}} \ .$$

Let m be even and α be an element of order $p = 2^m - 1$ in $\mathrm{GF}(2^m)$. Then the m-sequence $\{s_t\}$ of length $p = 2^m - 1$ can be written in terms of the trace mapping as

$$s_t = \mathrm{Tr}_m(\alpha^t) \ .$$

Let $\beta = \alpha^{2^{m/2}+1}$ be an element of order $2^{m/2} - 1$. The sequence $\{u_t\}$ of length $2^{m/2} - 1$ (which is used in the construction of the well known Kasami family) is defined by

$$u_t = \mathrm{Tr}_{m/2}(\beta^t) \ .$$

In this paper, we consider the cross correlation between the m-sequences $\{s_t\}$ and $\{v_t\} = \{u_{dt}\}$ at shift τ defined by

$$C_d(\tau) = \sum_{t=0}^{p-1} (-1)^{s_t + v_{t+\tau}} \ , \tag{1}$$

where $\gcd(d, 2^{m/2} - 1) = 1$ and $\tau = 0, 1, \ldots, 2^{m/2} - 2$. Using the trace representation, Ness and Helleseth [4] showed that the set of values of $C_d(\tau) + 1$ for $\tau = 0, 1, \ldots, 2^{m/2} - 2$ is equal to the set of values of

$$S(a) = \sum_{x \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(ax) + \mathrm{Tr}_{m/2}(x^{d(2^{m/2}+1)})} \tag{2}$$

when $a \in \mathrm{GF}(2^{m/2})^*$.

The main result of this paper is formulated in the following corollary that gives a four-valued cross-correlation function between new pairs of m-sequences of different lengths.

Corollary 1 *Let $m = 2nk$ and $d = \frac{2^{nk}+1}{2^k+1}$, where $n > 2$ is odd and $k > 1$. Then the cross-correlation function $C_d(\tau)$ has the following distribution:*

$$\begin{array}{lll} -1 - 2^{(n+1)k} & \textit{occurs} & \frac{2^{(n-1)k}-1}{2^{2k}-1} \quad \textit{times} \ , \\ -1 - 2^{nk} & \textit{occurs} & \frac{(2^{nk}-1)(2^{k-1}-1)}{2^k-1} \quad \textit{times} \ , \\ -1 & \textit{occurs} & 2^{(n-1)k} - 1 \quad \textit{times} \ , \\ -1 + 2^{nk} & \textit{occurs} & \frac{(2^{nk}+1)2^{k-1}}{2^k+1} \quad \textit{times} \ . \end{array}$$

The result will be proved in a series of lemmas and propositions. The outline of the proof is as follows. Determining the set of values of $C_d(\tau) + 1$ for $\tau = 0, 1, \ldots, 2^{nk} - 2$ is equivalent to finding the set of values of $S(a)$ in (2) for $a \in \mathrm{GF}(2^{nk})^*$. Furthermore, we show that

$$S(a) = \frac{1}{2^k + 1} \sum_{i=0}^{2^k} S_i(a) \ ,$$

where $S_i(a)$ are defined by

$$S_j(a) = \sum_{y \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(r^j a y^{2^k+1}) + \mathrm{Tr}_{nk}(y^{2^{nk}+1})} \quad \text{and}$$

$$S_{2^k+1-j}(a) = \sum_{y \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(r^{-j} a y^{2^k+1}) + \mathrm{Tr}_{nk}(y^{2^{nk}+1})}$$

for $j = 0, 1, \ldots, 2^{k-1}$ and with $r = \alpha^{(2^{nk}-1)2^{k-1}}$.

We determine $S_0(a)$ exactly in Corollary 4 and find $S_i(a)^2$ in Lemma 4. Since $S(a)$ is an integer, we can resolve the sign ambiguity of all $S_i(a)$ for $i = 1, 2, \ldots, 2^k$. In order to determine $S_0(a)$, we need to consider zeros in $\mathrm{GF}(2^{nk})$ of the affine polynomial

$$A_a(x) = a^{2^k} x^{2^{2k}} + x^{2^k} + ax + c \ ,$$

where $c \in \mathrm{GF}(2^k)$ and $\mathrm{Tr}_k(c) = 1$. To determine $S_i(a)^2$ for $1 = 1, 2, \ldots, 2^k$, we need to consider zeros in $\mathrm{GF}(2^{2nk})$ of the linearized polynomial

$$L_a(z) = z^{2^{(n+1)k}} + r^{2^k} a^{2^k} z^{2^{2k}} + raz \ ,$$

where n is odd, $a \in \mathrm{GF}(2^{nk})$ and $r \in \mathrm{GF}(2^{2nk})^*$ with $r^{2^{nk}+1} = 1$ but $r^{\frac{2^{nk}+1}{2^k+1}} \neq 1$.

When finding the complete cross-correlation distribution, we make use of the following lemma from [4].

Lemma 1 ([4]) *For any decimation d with $\gcd(d, 2^{nk}-1) = 1$ the sum of the cross-correlation values defined in (1) for $m = 2nk$ is equal to*

$$\sum_{\tau=0}^{2^{nk}-2} C_d(\tau) = 1 \ .$$

3 The Affine Polynomial $A_a(x)$

In this section, we consider zeros in $\mathrm{GF}(2^{nk})$, with $n > 2$, of the affine polynomial

$$A_a(x) = a^{2^k} x^{2^{2k}} + x^{2^k} + ax + c \ , \tag{3}$$

where $a \in \mathrm{GF}(2^{nk})$ and $c \in \mathrm{GF}(2^k)$. Some additional conditions on the parameters will be imposed later. The distribution of zeros in $\mathrm{GF}(2^{nk})$ of (3) will determine to a large extent the distribution of our cross-correlation function. It is clear that $A_a(x)$ does not have multiple roots if $a \neq 0$.

We introduce a particular sequence of polynomials over $\mathrm{GF}(2^{nk})$ that will play a crucial role when finding zeros of (3). First, for any $v \in \mathrm{GF}(2^{nk})$ denote $v_i = v^{2^{ik}}$ for $i = 0, \ldots, n-1$ so $A_a(x) = a_1 x_2 + x_1 + a_0 x_0 + c$. Let

$$\begin{aligned} B_1(x) &= 1 \ , \\ B_2(x) &= 1 \ , \\ B_{i+2}(x) &= B_{i+1}(x) + x_i B_i(x) \quad \text{for} \quad 1 \leq i \leq n-1 \ . \end{aligned} \tag{4}$$

Observe the following recursive identity that can be seen as an equivalent definition of $B_i(x)$

$$B_{i+2}(x) = B_{i+1}^{2^k}(x) + x_1 B_i^{2^{2k}}(x) \quad \text{for} \quad 1 \leq i \leq n-1 \ . \tag{5}$$

We prove it using induction on i. For $i = 1$ and $i = 2$ this fact is easily checked taking the definition. Assuming this identity holds for $i < t$ we get for $i = t > 2$

$$\begin{aligned} B_{t+2}(x) &\overset{(4)}{=} B_{t+1}(x) + x_t B_t(x) \\ &= B_t^{2^k}(x) + x_1 B_{t-1}^{2^{2k}}(x) + x_t B_{t-1}^{2^k}(x) + x_t x_1 B_{t-2}^{2^{2k}}(x) \\ &= \left(B_t(x) + x_{t-1} B_{t-1}(x)\right)^{2^k} + x_1 \left(B_{t-1}(x) + x_{t-2} B_{t-2}(x)\right)^{2^{2k}} \\ &\overset{(4)}{=} B_{t+1}^{2^k}(x) + x_1 B_t(x)^{2^{2k}} \ . \end{aligned}$$

We also define polynomials $Z_n(x)$ over $\mathrm{GF}(2^{nk})$ as

$$Z_n(x) = B_{n+1}(x) + x B_{n-1}^{2^k}(x) \ . \tag{6}$$

The following lemma describes zeros of $B_n(x)$ and $Z_n(x)$ in $\mathrm{GF}(2^{nk})$.

Lemma 2 *For any $v \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^k)$ let*

$$V = \frac{v_0^{2^{2k}+1}}{(v_0+v_1)^{2^k+1}} \quad . \tag{7}$$

Then for $n > 1$

$$B_n(V) = \frac{\mathrm{Tr}_k^{nk}(v_0)}{(v_1+v_2)} \prod_{j=2}^{n-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jk}} \quad .$$

If $n > 1$ is odd (resp. $n > 2$ is even) then the total number of distinct zeros of $B_n(x)$ in $\mathrm{GF}(2^{nk})$ is equal to $\frac{2^{(n-1)k}-1}{2^{2k}-1}$ (resp. $\frac{2^{(n-1)k}-2^k}{2^{2k}-1}$). Moreover, polynomial $B_n(x)$ splits in $\mathrm{GF}(2^{nk})$, all its zeros have the form of (7) with $\mathrm{Tr}_k^{nk}(v_0) = 0$ and occur with multiplicity 2^k.

Proof. First, note that $v \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^k)$ if and only if $v_0 \neq v_1$ which guarantees that the denominator in (7) and in the above identity for $B_n(V)$ is not zero. Now, using induction on i we prove that

$$B_i(V) = \frac{\sum_{j=1}^{i} v_j}{(v_1+v_2)} \prod_{j=2}^{i-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jk}} \tag{8}$$

for $2 \leq i \leq n+1$. For $i = 2$ and $i = 3$ this identity is easily checked using the definition (4) of $B_i(x)$ (for $i = 2$, we assume the product over the empty set to be equal to 1). Assuming this identity holds for $i < t$ we get for $i = t > 3$

$$\begin{aligned}
B_t(V) &\overset{(4)}{=} B_{t-1}(V) + V_{t-2}B_{t-2}(V) \\
&= \frac{\sum_{j=1}^{t-1} v_j}{(v_1+v_2)} \prod_{j=2}^{t-2} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jk}} + \frac{v_{t-2}^{2^{2k}+1} \sum_{j=1}^{t-2} v_j}{(v_{t-2}+v_{t-1})^{2^k+1}(v_1+v_2)} \prod_{j=2}^{t-3} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jk}} \\
&= \frac{\left((v_{t-1}+v_t)\sum_{j=1}^{t-1} v_j + v_t \sum_{j=1}^{t-2} v_j\right) \prod_{j=2}^{t-2} v_0^{2^{jk}}}{(v_1+v_2)\prod_{j=2}^{t-1}(v_0+v_1)^{2^{jk}}} \\
&= \frac{\sum_{j=1}^{t} v_j}{(v_1+v_2)} \prod_{j=2}^{t-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jk}} \quad .
\end{aligned}$$

It remains to note that for $i = n$, in $\mathrm{GF}(2^{nk})$ we have $\sum_{j=1}^{n} v_j = \mathrm{Tr}_k^{nk}(v_0)$.

Obviously, $B_n(V) = 0$ if and only if $\mathrm{Tr}_k^{nk}(v_0) = 0$ which is equivalent to $v_0 = u + u^{2^k}$ for some $u \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^{2k})$ (since $v_0 \in \mathrm{GF}(2^k)$ if and only if the corresponding $u \in \mathrm{GF}(2^{2k})$). It follows from the proof of Proposition 3 that the mapping from $u \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^{2k})$ via $v_0 = u + u^{2^k}$ to $V \in \mathrm{GF}(2^{nk})^*$ defined

by (7) is $(2^{3k}-2^k)$-to-1. Therefore, we have found $\frac{|\mathrm{GF}(2^{nk})\setminus\mathrm{GF}(2^{2k})|}{2^{3k}-2^k}$ distinct zeros of $B_n(x)$ in $\mathrm{GF}(2^{nk})$ and if n is odd (resp. n is even) then this number is equal to $\frac{2^{(n-1)k}-1}{2^{2k}-1}$ (resp. $\frac{2^{(n-1)k}-2^k}{2^{2k}-1}$).

It is easy to check by induction that if i is odd (resp. i is even) then the algebraic degree of polynomials $B_i(x)$ is equal to $\frac{2^{ik}-2^k}{2^{2k}-1}$ (resp. $\frac{2^{ik}-2^{2k}}{2^{2k}-1}$) since

$$\deg B_{i+2}(x) = \max\{\deg B_{i+1}(x), 2^{ik} + \deg B_i(x)\} = 2^{ik} + \deg B_i(x) \ .$$

Further, if we define the sequence of polynomials $B'_i(x)$ for $i = 1, \ldots, n$ with $B'_1(x) = B'_2(x) = 1$ and $B'_{i+2}(x) = B'_{i+1}(x) + x_{i-1}B'_i(x)$ then $B_i(x) = B'_i(x)^{2^k}$ for $i = 1, \ldots, n$. Therefore, all zeros of $B_n(x)$ having the form of (7) with $\mathrm{Tr}_k^{nk}(v_0) = 0$ have multiplicity at least 2^k. Finally, note that the number of these zeros multiplied by 2^k is equal to the degree of $B_n(x)$. □

Corollary 2 *For any $n > 1$, polynomial $Z_n(x)$ splits in $\mathrm{GF}(2^{nk})$ with all its zeros having the form of (7) and without multiple roots. If n is odd (resp. n is even) then the total number of zeros of $Z_n(x)$ in $\mathrm{GF}(2^{nk})$ is equal to $\frac{2^{(n+1)k}-2^{2k}}{2^{2k}-1}$ (resp. $\frac{2^{(n+1)k}-2^k}{2^{2k}-1}$).*

Proof. Using (8), it can be verified directly that $B_{n+1}(V) = VB_{n-1}^{2^k}(V)$ for any $V \in \mathrm{GF}(2^{nk})$ having the form of (7) (the case $n = 2$ is easily checked having the definition of $B_i(x)$). Also, using the fact from the latest proof, we conclude that $\deg Z_n(x) = \deg B_{n+1}(x)$ and is equal to $\frac{2^{(n+1)k}-2^{2k}}{2^{2k}-1}$ (resp. $\frac{2^{(n+1)k}-2^k}{2^{2k}-1}$) if n is odd (resp. n is even). Denote $S = \{x \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^k) \mid \mathrm{Tr}_k^{nk}(x) \neq 0\}$. It follows from the proof of Proposition 2 that the mapping from $v \in S$ to $V \in \mathrm{GF}(2^{nk})^*$ defined by (7) is (2^k-1)-to-1. Recalling the corresponding fact from the latest proof, we conclude that the total number of distinct values of V obtained by (7) is equal to $\frac{|\mathrm{GF}(2^{nk})\setminus\mathrm{GF}(2^{2k})|}{2^{3k}-2^k} + \frac{|S|}{2^k-1}$ being identical to the degree of $Z_n(x)$. Note that two different values of $v \in \mathrm{GF}(2^{nd}) \setminus \mathrm{GF}(2^d)$ with zero and nonzero trace in $\mathrm{GF}(2^d)$ can not map to the same value V using (7) since $C_n(V) = 0$ if and only if the trace of the corresponding v is also equal zero. □

Corollary 3 *For any $V \in \mathrm{GF}(2^{nk})$ having the form of (7) with $n > 2$ and $\mathrm{Tr}_k^{nk}(v_0) \neq 0$ we have*

$$\mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(V)}{B_n^{2^k+1}(V)}\right) = 0 = \mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(V)B_{n+1}(V)}{B_n^{2^k+1}(V)}\right) \ ,$$

where the second identity holds if and only if n is odd.

Proof. Using (8), it can be verified directly that

$$\frac{B_{n-1}^{2^k}(V)}{B_n^{2^k+1}(V)} = \mathrm{N}_k^{nk}\left(1+\frac{v_1}{v_0}\right)\frac{v_1\sum_{j=2}^n v_j}{\mathrm{Tr}_k^{nk}(v_0)^2} \qquad \text{and}$$
$$\frac{B_{n-1}^{2^k}(V)B_{n+1}(V)}{B_n^{2^k+1}(V)} = \frac{\left(v_1+\mathrm{Tr}_k^{nk}(v_0)\right)\sum_{j=2}^n v_j}{\mathrm{Tr}_k^{nk}(v_0)^2}$$

for any $V \in \mathrm{GF}(2^{nk})$ having the form of (7) and $n > 2$. Now note that

$$\mathrm{Tr}_k^{nk}\Big(v_1\sum_{j=2}^n v_j\Big) = \mathrm{Tr}_k^{nk}\left(v_1\mathrm{Tr}_k^{nk}(v_0)+v_1^2\right) = \mathrm{Tr}_k^{nk}(v_0)^2 + \mathrm{Tr}_k^{nk}(v_0^2) = 0$$

and thus,

$$\mathrm{Tr}_k^{nk}\Big(\left(v_1+\mathrm{Tr}_k^{nk}(v_0)\right)\sum_{j=2}^n v_j\Big) = \mathrm{Tr}_k^{nk}(v_0)\mathrm{Tr}_k^{nk}\left((\mathrm{Tr}_k^{nk}(v_0)+v_1)\right) = 0$$

if n is odd (and equal to $\mathrm{Tr}_k^{nk}(v_0)^2 \neq 0$ if n is even). □

Polynomials $B_i(x)$ can be interpreted as the determinant of three-diagonal symmetric matrices (note a comprehensive study of these matrices in [9]). Indeed, for $j \leq i$ let $\Delta_x(j,i)$ denote the determinant of matrix D_x of size $i-j+2$ that contains ones on the main diagonal and with $D_x(t,t+1) = D_x(t+1,t) = x_{j+t-1}$ for $t = 1,\ldots,i-j+1$, where the indices of x_i are reduced modulo n. Expanding the determinant of D_x by minors along the last row we obtain

$$\Delta_x(j,i) = \Delta_x(j,i-1) + x_i^2\Delta_x(j,i-2) \tag{9}$$

assuming $\Delta_x(j,i) = 1$ if $i-j \in \{-2,-1\}$. Comparing the latter recursive identity with (4) it is easy to see that

$$\Delta_x(1,i) = B_{i+2}^2(x) \ . \tag{10}$$

Moreover, from the definition of the determinant it also follows that

$$\Delta_x(1,i)^{2^{tk}} = \Delta_x(1+t,i+t) \quad \text{for} \quad 0 \leq t \leq n-1 \ . \tag{11}$$

We will need the following result that can be obtained combining Theorems 5.6 and 6.4 in [10].

Theorem 1 ([10]) *Take polynomials over* $\mathrm{GF}(2^{nk})$

$$f(x) = x^{2^k+1} + b^2x + b^2 \quad \textit{and} \quad g(x) = b^{-1}f(bx^{2^k-1}) = b^{2^k}x^{2^{2k}-1} + b^2x^{2^k-1} + b$$

with $b \neq 0$. *Then exactly one of the following holds*

(i) $f(x)$ *has none or two zeros in* $\mathrm{GF}(2^{nk})$ *and* $g(x)$ *has none zeros in* $\mathrm{GF}(2^{nk})$*;*

(ii) $f(x)$ *has one zero in* $\mathrm{GF}(2^{nk})$ *and* $g(x)$ *has* 2^k-1 *zeros in* $\mathrm{GF}(2^{nk})$*;*

(iii) $f(x)$ *has* 2^k+1 *zeros in* $\mathrm{GF}(2^{nk})$ *and* $g(x)$ *has* $2^{2k}-1$ *zeros in* $\mathrm{GF}(2^{nk})$*.*

Let N_i *denote the number of* $b \in \mathrm{GF}(2^{nk})^*$ *such that* $g(x)=0$ *has exactly* i *roots in* $\mathrm{GF}(2^{nk})$*. Then the following distribution holds for* n *odd (resp.* n *even)*

$$\begin{array}{lcll} N_0 & = & \frac{2^{(n+2)k}-2^{(n+1)k}-2^{nk}+1}{2^{2k}-1} & (resp.\ \frac{2^{(n+2)k}-2^{(n+1)k}-2^{nk}-2^{2k}+2^k+1}{2^{2k}-1}) \ , \\ N_{2^k-1} & = & 2^{(n-1)k}-1 & (resp.\ 2^{(n-1)k}) \ , \\ N_{2^{2k}-1} & = & \frac{2^{(n-1)k}-1}{2^{2k}-1} & (resp.\ \frac{2^{(n-1)k}-2^k}{2^{2k}-1}) \ . \end{array}$$

Let

$$M_i = \{a \mid a \neq 0, A_a(x) \text{ has exactly } i \text{ zeros in } \mathrm{GF}(2^{nk})\} \ .$$

Obviously, either $A_a(x)$ has no zeros in $\mathrm{GF}(2^{nk})$ or it has exactly the same number of zeros as its linearized homogeneous part that is $l_a(x) = a_1 x^{2^{2k}} + x^{2^k} + a_0 x$. The zeros in $\mathrm{GF}(2^{nk})$ of $l_a(x)$ form a vector subspace over $\mathrm{GF}(2^k)$. In the following propositions, we prove that $A_a(x)$ always has a zero in $\mathrm{GF}(2^{nk})$ so $A_a(x)$ and $l_a(x)$ have the same number of zeros in $\mathrm{GF}(2^{nk})$ that can be equal to $1, 2^k$ or 2^{2k}. Assume $a \neq 0$, then dividing $l_a(x)$ by $a_0 a_1 x$ (we remove one zero $x=0$) and then substituting x with $a_0^{-1}x$ leads to $a_1^{-2^k} x^{2^{2k}-1} + a_1^{-2} x^{2^k-1} + a_1^{-1}$ which has the form of polynomial $g(x)$ from Theorem 1 taking $b = a_1^{-1}$ (note a 1-to-1 correspondence between a and b). Thus, $|M_i| = N_{i-1}$ for $i \in \{1, 2^k, 2^{2k}\}$.

Proposition 1 *For any* $a \in \mathrm{GF}(2^{nk})^*$*, polynomial* $A_a(x)$ *has exactly one zero in* $\mathrm{GF}(2^{nk})$ *if and only if* $Z_n(a) \neq 0$*. Moreover, this zero is equal to* $\mathcal{V}_a = cB_n(a)/Z_n(a)$ *and* $\mathrm{Tr}_{nk}(\mathcal{V}_a) = \mathrm{Tr}_k(nc)$*. Also if* n *is odd (resp.* n *is even) then*

$$|M_1| = \frac{2^{(n+2)k} - 2^{(n+1)k} - 2^{nk} + 1}{2^{2k}-1} \ (resp.\ \frac{2^{(n+2)k} - 2^{(n+1)k} - 2^{nk} - 2^{2k} + 2^k + 1}{2^{2k}-1}) \ .$$

Proof. We start with proving that $cB_n(a)/Z_n(a)$ indeed is a zero of $A_a(x)$ if $Z_n(a) \neq 0$. First, for any $v \in \mathrm{GF}(2^{nk})$, using both recursive definitions of $B_n(x)$

$$\begin{aligned} Z_n^{2^k}(v) &\overset{(6)}{=} B_{n+1}^{2^k}(v) + v_1 B_{n-1}^{2^{2k}}(v) \\ &\overset{(4)}{=} B_n^{2^k}(v) + v_0 B_{n-1}^{2^k}(v) + v_1 B_{n-1}^{2^{2k}}(v) \\ &\overset{(5)}{=} B_{n+1}(v) + v_0 B_{n-1}^{2^k}(v) \\ &\overset{(6)}{=} Z_n(v) \end{aligned}$$

and thus, $Z_n(v) \in \mathrm{GF}(2^k)$. Therefore,

$$\begin{aligned} A_a(\mathcal{V}_a) &= \frac{c}{Z_n(a)}\left(a_1 B_n^{2^{2k}}(a) + B_n^{2^k}(a) + a_0 B_n(a) + Z_n(a)\right) \qquad (12)\\ &\overset{(4)}{=} \frac{c}{Z_n(a)}\left(a_1 B_{n-1}^{2^{2k}}(a) + a_1 a_0 B_{n-2}^{2^{2k}}(a) + B_n^{2^k}(a) + a_0 B_n(a) + Z_n(a)\right)\\ &\overset{(5)}{=} \frac{c}{Z_n(a)}\left(B_{n+1}(a) + a_0 B_{n-1}^{2^k}(a) + Z_n(a)\right) = 0 \ . \end{aligned}$$

Now we show that in our case $\mathcal{V}_a$ is the only zero of $A_a(x)$. Taking equation $A_a(x) = 0$ and all its 2^{ik} powers we obtain n equations

$$A_a^{2^{ik}}(x) = a_{i+1}x_{i+2} + x_{i+1} + a_i x_i + c = 0 \quad \text{for} \quad i = 0, \ldots, n-1 \ ,$$

where all indices are calculated modulo n. If x_i $(i = 0, \ldots, n-1)$ are considered as independent variables then the obtained system of n linear equations with n unknowns has the following matrix with the antidiagonal structure

$$\begin{pmatrix} 0 & 0 & \cdots & a_1 & 1 & a_0 \\ 0 & & \iddots & 1 & a_1 & 0 \\ \vdots & \iddots & \iddots & \iddots & \iddots & \vdots \\ a_{n-2} & 1 & \iddots & & & 0 \\ 1 & a_{n-2} & \iddots & & 0 & a_{n-1} \\ a_{n-1} & 0 & \cdots & 0 & a_0 & 1 \end{pmatrix} . \qquad (13)$$

Let the columns of (13) be numbered from 1 to n. Permuting the columns in (13) (reorder them as $n-1, n-2, \ldots, 1, n$) we obtain the symmetric three-diagonal cyclic matrix $\mathcal{M}_n$ containing ones on the main diagonal, with $\mathcal{M}_n(i, i+1) = \mathcal{M}_n(i+1, i) = a_i$ for $i = 1, \ldots, n-1$ and with corner elements $\mathcal{M}_n(1, n) = \mathcal{M}_n(n, 1) = a_0$. If $\boldsymbol{x} = (x_1, \ldots, x_{n-1}, x_0)^{\mathrm{T}}$ and $\boldsymbol{c} = (c, \ldots, c)^{\mathrm{T}}$ then the system has the following matrix representation

$$\mathcal{M}_n \boldsymbol{x} = \boldsymbol{c} \ . \qquad (14)$$

The determinant of (13) is equal to the determinant of $\mathcal{M}_n$ and can be computed expanding the latter by minors along the last row. Doing this it is easy to see that

$$\begin{aligned} \det \mathcal{M}_n &= \Delta_a(1, n-2) + a_{n-1}(a_{n-1}\Delta_a(1, n-3) + a_0 \ldots a_{n-2}) \\ &\qquad + a_0(a_0 \Delta_a(2, n-2) + a_1 \ldots a_{n-1}) \\ &\overset{(10,11)}{=} B_n^2(a) + a_{n-1}^2 B_{n-1}^2(a) + (a_0 B_{n-1}^{2^k}(a))^2 \\ &\overset{(4)}{=} B_{n+1}^2(a) + (a_0 B_{n-1}^{2^k}(a))^2 \\ &\overset{(6)}{=} Z_n^2(a) \ . \end{aligned}$$

Thus, if $Z_n(a) \neq 0$ then (14) has exactly one solution. Now note that every $v \in \mathrm{GF}(2^{nk})$ with $A_a(v) = 0$ provides a solution to the system given by $v_i = v^{2^{ik}}$ for $i = 0, \ldots, n-1$. Therefore, if $Z_n(a) \neq 0$ then $A_a(x)$ has at most one zero.

Using Corollary 2, we can obtain the number of $a \in \mathrm{GF}(2^{nk})^*$ such that $Z_n(a) \neq 0$ (note that $Z_n(0) = 1$). Observe that this number is identical to N_0 from Theorem 1 that is equal to the number of $a \in \mathrm{GF}(2^{nk})^*$ such that $l_a(x) = 0$ has exactly one root in $\mathrm{GF}(2^{nk})$ (see explanations following Theorem 1). Therefore, if $A_a(x)$ has exactly one zero in $\mathrm{GF}(2^{nk})$ then its homogeneous part $l_a(x)$ has the same number of zeros and so a is necessarily such that $Z_n(a) \neq 0$.

Finally, to prove the trace identity for $\mathcal{V}_a$ first note that for any $v \in \mathrm{GF}(2^{nk})$

$$\begin{aligned} \mathrm{Tr}_k^{nk}(B_n(v) + Z_n(v)) &\overset{(6)}{=} \mathrm{Tr}_k^{nk}\left(B_n(v) + B_{n+1}(v) + v_0 B_{n-1}^{2^k}(v)\right) \\ &\overset{(4)}{=} \mathrm{Tr}_k^{nk}\left(B_n(v) + B_n(v) + v_{n-1}B_{n-1}(v) + v_0 B_{n-1}^{2^k}(v)\right) \\ &= \mathrm{Tr}_k^{nk}\left(v_{n-1}B_{n-1}(v) + (v_{n-1}B_{n-1}(v))^{2^k}\right) = 0 \ . \end{aligned} \tag{15}$$

Therefore, since c and $Z_n(v)$ are both in $\mathrm{GF}(2^k)$, then

$$\begin{aligned} \mathrm{Tr}_{nk}(\mathcal{V}_v) &= \mathrm{Tr}_{nk}\left(c + c\,\frac{B_n(v) + Z_n(v)}{Z_n(v)}\right) \\ &= \mathrm{Tr}_k(nc) + \mathrm{Tr}_k\left(\frac{c}{Z_n(v)}\,\mathrm{Tr}_k^{nk}(B_n(v) + Z_n(v))\right) \\ &= \mathrm{Tr}_k(nc) \ . \end{aligned}$$

This completes the proof. □

Proposition 2 *Let n be odd and take any $a \in \mathrm{GF}(2^{nk})^*$. Then polynomial $A_a(x)$ has exactly 2^k zeros in $\mathrm{GF}(2^{nk})$ if and only if $Z_n(a) = 0$ and $B_n(a) \neq 0$. Moreover, these zeros are the following*

$$v_\mu = c \sum_{i=0}^{\frac{n-1}{2}} \frac{B_{n-1}^{2^{(2i+1)k}}(a)}{B_n^{2^{(2i+1)k}+2^{2ik}-1}(a)} + \mu B_n(a)$$

with $\mu \in \mathrm{GF}(2^k)$ and for each zero of this type $\mathrm{Tr}_{nk}(v_\mu) = 0$. Also $|M_{2^k}| = 2^{(n-1)k} - 1$.

Proof. First, we consider $l_a(x) = a_1 x^{2^{2k}} + x^{2^k} + a_0 x$ being the linearized homogeneous part of $A_a(x)$, and prove that it has exactly 2^k zeros in $\mathrm{GF}(2^{nk})$ if and only if $Z_n(a) = 0$ and $B_n(a) \neq 0$.

Assume that $Z_n(a) = 0$ and $B_n(a) \neq 0$. Then, by (12),

$$a_1 B_n^{2^{2k}}(a) + B_n^{2^k}(a) + a_0 B_n(a) = 0 \tag{16}$$

which means that all 2^k distinct values $\mu B_n(a)$ for $\mu \in \mathrm{GF}(2^k)$ are zeros of $l_a(x)$. It is not difficult to see that in our case $l_a(x)$ can not have more than 2^k zeros in $\mathrm{GF}(2^{nk})$. Indeed, consider matrix $\mathcal{M}_n$ of the system of n linear equations (14) with $c = 0$. Note that $\det \mathcal{M}_n = Z_n^2(a) = 0$ and a principal submatrix obtained by deleting the last column and the last row from $\mathcal{M}_n$ is nonsingular with the determinant $\Delta_a(1, n-2) = B_n^2(a) \neq 0$ (see (10)). Therefore, applying equivalent row transformations to $\mathcal{M}_n$ we can obtain a matrix containing a nonsingular diagonal submatrix lying in the first $n-1$ columns and rows. Thus, the equation given by the first row of this equivalent matrix is nonzero and has degree 2^k. We conclude that homogeneous system (14) can not have more than 2^k solutions and the same holds for the equation $l_a(x) = 0$.

Now we prove the converse implication. Assume that $l_a(x)$ has exactly 2^k zeros in $\mathrm{GF}(2^{nk})$. Here we use the technique found by Bluher [10] for counting the number of $b \in \mathrm{GF}(2^{nk})^*$ for which $f_b(y) = y^{2^k+1} + by + b$ has exactly one zero in $\mathrm{GF}(2^{nk})$. Denote $S = \{x \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^k) \mid \mathrm{Tr}_k^{nk}(x) \neq 0\}$. For any $v \in S$ define $r = v^{1-2^k} + 1 \in \mathrm{GF}(2^{nk}) \setminus \{0, 1\}$ and corresponding $b = \frac{r^{2^k+1}}{r+1} \neq 0$. Obviously, such an r is a zero of $f_b(y)$. Note that

$$b = \frac{r^{2^k+1}}{r+1} = v^{2^k-1}(v^{1-2^k}+1)^{2^k+1} = \frac{(v+v^{2^k})^{2^k+1}}{v^{2^{2k}+1}} = V^{-1} \ , \qquad (17)$$

where V comes from (7). Then, by Lemma 2 and Corollary 2, $B_n(b^{-1}) \neq 0$ and $Z_n(b^{-1}) = 0$. By the implication already proved, $l_{b^{-1}}(x)$ has exactly 2^k zeros in $\mathrm{GF}(2^{nk})$. Multiplying the latter polynomial by $b_0 b_1 x^{-1}$ (we remove one zero $x = 0$) and then substituting x with $b_0 y$ leads to $b_1^{2^k} y^{2^{2k}-1} + b_1^2 y^{2^k-1} + b_1$ with $2^k - 1$ zeros and having the form of polynomial $g(x)$ from Theorem 1. Thus, by (ii) in this theorem, $f_b(y)$ (as well as $f_{b^{2^{l+1}}}(y)$) has exactly one zero in $\mathrm{GF}(2^{nk})$.

Now we prove that function (17) that maps every $v \in S$ to $b \in \mathrm{GF}(2^{nk})^*$ is a (2^k-1)-to-1 mapping. First, note that (2^k-1)-power is a (2^k-1)-to-1 mapping of S to $\mathrm{GF}(2^{nk})^*$. Indeed, if $x \in S$ and $x^{2^k-1} = t$ then the latter identity holds for all distinct $\delta x \in S$ with $\delta \in \mathrm{GF}(2^k)^*$ since $\mathrm{Tr}_k^{nk}(\delta x) = \delta \mathrm{Tr}_k^{nk}(x) \neq 0$ and $\delta x \notin \mathrm{GF}(2^k)$. Thus, every $r = v^{1-2^k} + 1$ is obtained from $2^k - 1$ different values of v. Finally, the mapping from r to b is 1-to-1 since for the obtained b the equation $f_b(y) = 0$ has exactly one root r.

Therefore, taking all $v \in S$ and using (17), we obtain $|S|/(2^k-1)$ different values of $b \in \mathrm{GF}(2^{nk})^*$ and this number is equal to the total number of b such that $f_b(y)$ has exactly one zero (see Theorem 1). Therefore, these and only these values of b satisfying (17) result in the polynomials $f_b(y)$ having exactly one zero.

Dividing $l_a(x)$ by $a_0 a_1 x$ (we remove one zero $x = 0$) and then substituting x with $a_0^{-1} y$ leads to $a_1^{-2^k} y^{2^{2k}-1} + a_1^{-2} y^{2^k-1} + a_1^{-1}$ which has the form of polynomial $g(x)$ from Theorem 1 taking $b = a_1^{-1}$. Thus, $f_{a^{-1}}(y)$ (as well as $f_{a^{-2^{l+1}}}(y)$) has

exactly one zero in $\mathrm{GF}(2^{nk})$ and a^{-1} is obtained by (17). Therefore, by Lemma 2 and Corollary 2, $B_n(a) \neq 0$ and $Z_n(a) = 0$.

If $A_a(x)$ has exactly 2^k zeros in $\mathrm{GF}(2^{nk})$ then the same holds for its homogeneous part $l_a(x)$ and we already proved that in this case, $Z_n(a) = 0$ and $B_n(a) \neq 0$. Now we have to find a particular solution of $A_a(x) = 0$ assuming $Z_n(a) = 0$ and $B_n(a) \neq 0$. By Corollary 2, a has the form of (7) and, by Lemma 2, $\mathrm{Tr}_k^{nk}(v_0) \neq 0$. Using these facts and assuming that n is odd (note that the latter assumption is involved only at this stage), we compute

$$
\begin{aligned}
A_a\left(c\sum_{i=0}^{\frac{n-1}{2}}\frac{B_{n-1}^{2^{(2i+1)k}}(a)}{B_n^{2^{(2i+1)k}+2^{2ik}-1}(a)}\right) &= ca_1B_n^{2^{2k}}(a)\sum_{i=1}^{\frac{n-1}{2}}\frac{B_{n-1}^{2^{(2i+1)k}}(a)}{B_n^{2^{(2i+1)k}+2^{2ik}}(a)} \\
&+ ca_1B_n^{2^{2k}}(a)\frac{B_{n-1}^{2^{2k}}(a)}{B_n^{2^{2k}+2^k}(a)} + cB_n^{2^k}(a)\sum_{i=1}^{\frac{n-1}{2}}\frac{B_{n-1}^{2^{2ik}}(a)}{B_n^{2^{2ik}+2^{(2i-1)k}}(a)} \\
&+ cB_n^{2^k}(a)\frac{B_{n-1}^{2^k}(a)}{B_n^{2^k+1}(a)} + ca_0B_n(a)\sum_{i=0}^{\frac{n-1}{2}}\frac{B_{n-1}^{2^{(2i+1)k}}(a)}{B_n^{2^{(2i+1)k}+2^{2ik}}(a)} + c \\
&\overset{(16)}{=} cB_n^{2^k}(a)\sum_{i=0}^{\frac{n-1}{2}}\frac{B_{n-1}^{2^{(2i+1)k}}(a)}{B_n^{2^{(2i+1)k}+2^{2ik}}(a)} + cB_n^{2^k}(a)\sum_{i=1}^{\frac{n-1}{2}}\frac{B_{n-1}^{2^{2ik}}(a)}{B_n^{2^{2ik}+2^{(2i-1)k}}(a)} \\
&+ ca_0B_n(a)\frac{B_{n-1}^{2^k}(a)}{B_n^{2^k+1}(a)} + ca_1B_n^{2^{2k}}(a)\frac{B_{n-1}^{2^{2k}}(a)}{B_n^{2^{2k}+2^k}(a)} + c \\
&= cB_n^{2^k}(a)\mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(a)}{B_n^{2^k+1}(a)}\right) + c\frac{a_0B_{n-1}^{2^k}(a) + (a_0B_{n-1}^{2^k}(a))^{2^k}}{B_n^{2^k}(a)} + c \\
&\overset{(*)}{=} c\frac{(a_{n-1}B_{n-1}(a))^{2^k} + B_{n+1}^{2^k}(a)}{B_n^{2^k}(a)} + c \overset{(4)}{=} 0 \ ,
\end{aligned}
$$

where $(*)$ holds by Corollary 3 and since $B_{n+1}(a) = a_0B_{n-1}^{2^k}(a)$ resulting from (6) if $Z_n(a) = 0$.

Finally, to prove the trace identity for v_μ first note that, by (15), $\mathrm{Tr}_k^{nk}(B_n(a)+$

$Z_n(a)) = \mathrm{Tr}_k^{nk}(B_n(a)) = 0$ if $Z_n(a) = 0$. Further,

$$\begin{aligned}
\mathrm{Tr}_k^{nk}\left(\sum_{i=0}^{\frac{n-1}{2}} \frac{B_{n-1}^{2^{(2i+1)k}}(a)}{B_n^{2^{(2i+1)k}+2^{2ik}-1}(a)}\right) &= \sum_{j=0}^{n-1}\sum_{i=0}^{\frac{n-1}{2}} \frac{B_n^{2^{jk}}(a) B_{n-1}^{2^{(2i+j+1)k}}(a)}{B_n^{2^{(2i+j+1)k}+2^{(2i+j)k}}(a)} \\
= \sum_{j=0}^{n-1} \frac{B_{n-1}^{2^{(j+1)k}}(a)\sum_{i=0}^{\frac{n-1}{2}} B_n^{2^{(j-2i)k}}(a)}{B_n^{2^{(j+1)k}+2^{jk}}(a)} &= \mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(a)\sum_{i=0}^{\frac{n-1}{2}} B_n^{2^{(2i+1)k}}(a)}{B_n^{2^k+1}(a)}\right) \\
= \mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(a)\sum_{i=0}^{\frac{n-1}{2}} \left(B_{n+1}(a) + B_{n+1}^{2^k}(a)\right)^{2^{2ik}}}{B_n^{2^k+1}(a)}\right) & \\
= \mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(a)\left(\mathrm{Tr}_k^{nk}(B_{n+1}(a)) + B_{n+1}(a)\right)}{B_n^{2^k+1}(a)}\right) & \\
= \mathrm{Tr}_k^{nk}(B_{n+1}(a))\mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(a)}{B_n^{2^k+1}(a)}\right) + \mathrm{Tr}_k^{nk}\left(\frac{B_{n-1}^{2^k}(a)B_{n+1}(a)}{B_n^{2^k+1}(a)}\right) &= 0 \ ,
\end{aligned}$$

where the latest identity follows by Corollary 3.

The identity for $|M_{2^k}|$ follows from Theorem 1. □

Now we are left with the remaining case when $B_n(a) = 0$ (then, obviously, $Z_n(a) = 0$). In the following proposition, the "only if" part follows from Propositions 1 and 2. We provide this proof yet, independently of previous statements, since its major part contains the result used for proving the converse implication and also needed for proving the fact from Lemma 2.

Proposition 3 *Take any $a \in \mathrm{GF}(2^{nk})^*$. Then polynomial $l_a(x) = a_1 x^{2^{2k}} + x^{2^k} + a_0 x$ has exactly 2^{2k} zeros in $\mathrm{GF}(2^{nk})$ if and only if $B_n(a) = 0$.*

Proof. Assume that $l_a(x)$ has exactly 2^{2k} zeros in $\mathrm{GF}(2^{nk})$. Here we use the technique found by Bluher [10] for counting the number of $b \in \mathrm{GF}(2^{nk})^*$ for which $f_b(y) = y^{2^k+1} + by + b$ has 2^k+1 zeros in $\mathrm{GF}(2^{nk})$. Denote $G = \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^{2k})$. Take any $u \in \mathrm{GF}(2^{nk})$ such that $u \notin \mathrm{GF}(2^{2k})$ which implies $u^{2^{2k}} \neq u$ and $(u + u^{2^k})^{2^k} \neq u + u^{2^k}$ or, equivalently, $u + u^{2^k} \notin \mathrm{GF}(2^k)$. Now we can define $r = (u + u^{2^k})^{1-2^k} + 1 \in \mathrm{GF}(2^{nk}) \setminus \{0, 1\}$ and corresponding $b = \frac{r^{2^k+1}}{r+1} \neq 0$. Obviously, such an r is a zero of $f_b(y)$. Define also $r_0 = ru^{2^k-1}$ and $r_1 = r(u+1)^{2^k-1}$ and note that r, r_0 and r_1 are pairwise distinct. Further,

$$f_b(r_0) = r^{2^k+1}u^{2^{2k}-1} + bru^{2^k-1} + b = b((r+1)u^{2^{2k}} + ru^{2^k} + u)/u = 0$$

since $r(u + u^{2^k})^{2^k} = u + u^{2^{2k}}$ by the definition of r. Also, similarly, we get

$$f_b(r_1) = b((r+1)(u+1)^{2^{2k}} + r(u+1)^{2^k} + (u+1))/(u+1) = b(r+1+r+1)/(u+1) = 0 \ .$$

Thus, $f_b(y)$ with such a b has at least three zeros and, by Theorem 1, it has 2^k+1 zeros. Note that

$$b = \frac{r^{2^k+1}}{r+1} = (u+u^{2^k})^{2^k-1}((u+u^{2^k})^{1-2^k}+1)^{2^k+1} = \frac{(u+u^{2^{2k}})^{2^k+1}}{(u+u^{2^k})^{2^{2k}+1}} = V^{-1} \ , \ (18)$$

where V comes from (7) assuming $v = u + u^{2^k}$.

Now we prove that function (18) that maps every $u \in G$ to $b \in \mathrm{GF}(2^{nk})^*$ is a $(2^{3k}-2^k)$-to-1 mapping. First, note that $u+u^{2^k}$ is a 2^k-to-1 mapping onto $F = \{x \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^k) \mid \mathrm{Tr}_k^{nk}(x) = 0\}$. Further, (2^k-1)-power is a (2^k-1)-to-1 mapping of F to $\mathrm{GF}(2^{nk})^*$. Indeed, if $x \in F$ and $x^{2^k-1} = t$ then the latter identity holds for all distinct $\delta x \in F$ with $\delta \in \mathrm{GF}(2^k)^*$ since $\mathrm{Tr}_k^{nk}(\delta x) = \delta \mathrm{Tr}_k^{nk}(x) = 0$ and $\delta x \notin \mathrm{GF}(2^k)$. Thus, every $r = (u+u^{2^k})^{1-2^k}+1$ is obtained from $2^k(2^k-1)$ different values of u. Finally, the mapping from r to b is (2^k+1)-to-1 since for the obtained b the equation $f_b(y) = 0$ has (2^k+1) roots and every root r satisfies $(r+1)^{-1} \in F^{2^k-1}$. Indeed, let r, r_0 and r_1 be any distinct zeros of $f_b(y)$ (not necessarily the ones defined above) and define $u = (r+r_1)/(r_0+r_1)$. Note that

$$rr_0(r+r_0)^{2^k} = r_0 r^{2^k+1} + r r_0^{2^k+1} = r_0 b(r+1) + rb(r_0+1) = b(r+r_0)$$

and so $b = rr_0(r+r_0)^{2^k-1} = rr_1(r+r_1)^{2^k-1} = r_0 r_1 (r_0+r_1)^{2^k-1}$. Then

$$u^{2^{2k}-1} = (r_0/r)^{2^k+1} = (r_0+1)/(r+1) \neq 1$$

and thus, $u \in G$. The identity $(r+1)^{-1} = (u+u^{2^k})^{2^k-1} \in F^{2^k-1}$ follows from [10, Lemma 2.1].

Therefore, taking all $u \in G$ and using (18), we obtain $|G|/(2^{3k}-2^k)$ different values of $b \in \mathrm{GF}(2^{nk})^*$ and this number is equal to the total number of b such that $f_b(y)$ has 2^k+1 zeros (see Theorem 1). Therefore, these and only these values of b satisfying (18) result in the polynomials $f_b(y)$ having 2^k+1 zeros.

Dividing $l_a(x)$ by $a_0 a_1 x$ (we remove one zero $x = 0$) and then substituting x with $a_0^{-1}y$ leads to $a_1^{-2^k} y^{2^{2k}-1} + a_1^{-2} y^{2^k-1} + a_1^{-1}$ which has the form of polynomial $g(x)$ from Theorem 1 taking $b = a_1^{-1}$. Thus, $f_{a^{-1}}(y)$ (as well as $f_{a^{-2^{k+1}}}(y)$) has exactly 2^k+1 zeros in $\mathrm{GF}(2^{nk})$ and a^{-1} is obtained by (18). Therefore, by Lemma 2, $B_n(a) = 0$.

The converse implication is easy now. If $B_n(a) = 0$ then, by Lemma 2, a has the form of (7) with $v = u + u^{2^k}$ for some $u \in G$. Then the corresponding $b = a^{-1}$ has the form of (18) and, by the fact proved above, the polynomial $f_b(y)$ has 2^k+1 zeros which, by Theorem 1 (iii), is equivalent to $l_a(x)$ having 2^{2k} zeros. □

In the following proposition, we prove that $A_a(x) = 0$ always has a solution if n is odd and $\mathrm{Tr}_k(c) = 1$ (which is also valid for even n but this case is not relevant to the current paper).

Proposition 4 *Take any $a \in \mathrm{GF}(2^{nk})$, where n is odd and $c \in \mathrm{GF}(2^k)$ with $\mathrm{Tr}_k(c) = 1$. Then polynomial $A_a(x)$ has at least one zero in $\mathrm{GF}(2^{nk})$. Moreover, if $A_a(x)$ has exactly 2^{2k} zeros then $\mathrm{Tr}_{nk}(v) = 1$ for any $v \in \mathrm{GF}(2^{nk})$ with $A_a(v) = 0$ and $|M_{2^{2k}}| = \frac{2^{(n-1)k}-1}{2^{2k}-1}$.*

Proof. Take any pair $(a, v) \in \mathrm{GF}(2^{nk}) \times \mathrm{GF}(2^{nk})$ with $v \neq c$ such that $A_a(v) = 0$. Then, assuming $b = a\left(\frac{v}{v+c}\right)^{2^k+1}$, we obtain

$$\begin{aligned} A_b(v+c) &= a^{2^k}\frac{v^{2^{2k}+2^k}}{(v+c)^{2^k}} + (v+c)^{2^k} + a\frac{v^{2^k+1}}{(v+c)^{2^k}} + c \\ &= \frac{1}{(v+c)^{2^k}}\left(v^{2^k}(a^{2^k}v^{2^{2k}} + v^{2^k} + av) + c^2 + c(v^{2^k}+c)\right) = 0 \ . \end{aligned}$$

Since n is odd and $\mathrm{Tr}_k(c) = 1$, we obtain a 1-to-1 correspondence between two sets

$$\begin{aligned} S_0 &= \{(a, v) \mid v \neq c, A_a(v) = 0, \mathrm{Tr}_{nk}(v) = 0\} \quad \text{and} \\ S_1 &= \{(a, v) \mid v \neq c, A_a(v) = 0, \mathrm{Tr}_{nk}(v) = 1\} \end{aligned}$$

defined by $(a, v) \mapsto (b, v + c)$ with $b = a\left(\frac{v}{v+c}\right)^{2^k+1}$ and thus, $|S_0| = |S_1|$. Note that $A_a(c) = c(a^{2^k} + a) = 0$ if and only if $a \in \mathrm{GF}(2^k)$. Now, since $A_a(x)$ can have 0, 1, 2^k or 2^{2k} zeros, we can compute the following sum in two different ways

$$\begin{aligned} &\sum_{(a,v):\, A_a(v)=0} (-1)^{\mathrm{Tr}_{nk}(v)} = |S_0| - |S_1| - 2^k \\ &= (-1)^{\mathrm{Tr}_{nk}(c)} + \sum_{a \in M_1} (-1)^{\mathrm{Tr}_{nk}(\mathcal{V}_a)} + \sum_{a \in M_{2^k}} \sum_{v:\, A_a(v)=0} (-1)^{\mathrm{Tr}_{nk}(v)} + X \\ &= -1 - |M_1| + 2^k|M_{2^k}| + X \ , \end{aligned}$$

by Propositions 1 and 2, where $X = \sum_{a \in M_{2^{2k}}} \sum_{v:\, A_a(v)=0} (-1)^{\mathrm{Tr}_{nk}(v)}$. Then

$$X = -\frac{2^{2k}(2^{(n-1)k} - 1)}{2^{2k} - 1} = -2^{2k}(|\mathrm{GF}(2^{nk})^*| - |M_1| - |M_{2^k}|)$$

which holds if and only only if $|M_{2^{2k}}| = \frac{2^{(n-1)k}-1}{2^{2k}-1}$ and $\mathrm{Tr}_{nk}(v) = 1$ for any $v \in \mathrm{GF}(2^{nk})$ with $A_a(v) = 0$ and $a \in M_{2^{2k}}$. Since $|M_1| + |M_{2^k}| + |M_{2^{2k}}| = |\mathrm{GF}(2^{nk})^*|$ and $A_0(x)$ has a unique zero $x = c$, polynomial $A_a(x)$ has at least one zero in $\mathrm{GF}(2^{nk})$ for any $a \in \mathrm{GF}(2^{nk})$. □

4 The Linearized Polynomial $L_a(z)$

The distribution of the four-valued cross-correlation function to be determined in Section 5 depends on the detailed distribution of the number of zeros in $\mathrm{GF}(2^{2nk})$, with $n > 2$, of the linearized polynomial

$$L_a(z) = z^{2^{(n+1)k}} + r^{2^k} a^{2^k} z^{2^{2k}} + raz \ , \tag{19}$$

where n is odd, $a \in \mathrm{GF}(2^{nk})$ and $r \in \mathrm{GF}(2^{2nk})^*$ with $r^{2^{nk}+1} = 1$ but $r^{\frac{2^{nk}+1}{2^k+1}} \neq 1$. For the details on linearized polynomials in general, the reader is referred to Lidl and Niederreiter [11]. It is clear that $L_a(z)$ does not have multiple roots if $a \neq 0$. In the following propositions, we always take $L_a(z)$ defined in (19).

Define polynomials $Y_n(x)$ over $\mathrm{GF}(2^{nk})$ as

$$Y_n(x) = Z_n^2(x) + \mathrm{N}_k^{nk}(x)(\delta + \delta^{-1}) \ ,$$

where $\delta = r^{\frac{2^{nk}+1}{2^k+1}} \in \mathrm{GF}(2^{2k})$ is a $(2^k+1)^{\text{th}}$ root of unity over $\mathrm{GF}(2)$ and $Z_n(x)$ comes from (6). Also, for any $v \in \mathrm{GF}(2^{2nk})$ denote $v_i = v^{2^{ik}}$ for $i \geq 0$ so $L_a(z) = z_{n+1} + r_1 a_1 z_2 + r_0 a_0 z_0$. Finally, for $0 < j \leq i$ and $x \in \mathrm{GF}(2^{nk})$, let $D_x^{j,i}$ denote a three-diagonal matrix of size $i - j + 2$ that contains ones on the main diagonal and with

$$D_x^{j,i}(t, t+1) = r_{j+t}^{(-1)^{j+t-1}} x_{j+t} \quad \text{and} \quad D_x^{j,i}(t+1, t) = r_{j+t}^{(-1)^{j+t}} x_{j+t}$$

for $t = 0, \ldots, i-j$, where the indices of r, x and powers of r are reduced modulo n (the only exception is $j + t = n$ when $r_n^{(-1)^{n-1}} = r_0^{-1}$), rows and columns of $D_x^{j,i}$ are numbered from 0 to $i - j + 1$. The determinant of $D_x^{j,i}$, denoted as $\Delta'_x(j,i)$, can be computed expanding by minors along the last row to obtain

$$\Delta'_x(j,i) = \Delta'_x(j,i-1) + x_i^2 \Delta'_x(j,i-2)$$

assuming $\Delta'_x(j,i) = 1$ if $i - j \in \{-2, -1\}$. Comparing the latter recursive identity with (9) it is easy to see that

$$\Delta'_x(j,i) = \Delta_x(j,i) \ . \tag{20}$$

Zeros of $L_a(z)$ in $\mathrm{GF}(2^{2nk})$ form a vector space over $\mathrm{GF}(2^{2k})$. Since the degree of $L_a(z)$ is $2^{(n+1)k}$, the number of zeros is at most $2^{(n+1)k}$, and thus, the dimension of the vector space over $\mathrm{GF}(2^{2k})$ is at most $(n+1)/2$. Therefore, $L_a(z)$ has either $1, 2^{2k}, 2^{4k}, \ldots, 2^{(n+1)k}$ zeros in $\mathrm{GF}(2^{2nk})$. However, in Proposition 6 we prove that $L_a(z)$ can not have more than 2^{2k} zeros in $\mathrm{GF}(2^{2nk})$ and thus, the only possibilities are either 1 or 2^{2k} zeros.

Proposition 5 *For any $a \in \mathrm{GF}(2^{nk})^*$, if $Y_n(a) \neq 0$ then $L_a(z) = 0$ has exactly one root in $\mathrm{GF}(2^{2nk})$ that is equal to zero. In particular, if $Z_n(a) = 0$ ($Z_n(x)$ defined in (6)) then $L_a(z)$ has exactly one zero.*

Proof. Obviously, $L_a(0) = 0$ and we have to show that this is the only zero of $L_a(z)$ in $\mathrm{GF}(2^{2nk})$ if $Y_n(a) \neq 0$. Taking equation $L_a(z) = 0$ and all its 2^{2ik} powers we obtain n equations

$$L_a^{2^{2ik}}(x) = z_{n+2i+1} + r_{2i+1}a_{2i+1}z_{2i+2} + r_{2i}a_{2i}z_{2i} = 0 \quad \text{for} \quad i = 0, \ldots, n-1 \ ,$$

where all indices are calculated modulo $2n$. If z_{2i} $(i = 0, \ldots, n-1)$ are considered as independent variables then matrix $\mathcal{M}_n$ of the obtained system of n linear equations with n unknowns consists of three cyclic antidiagonals and

$$\begin{aligned} \mathcal{M}_n(i, (n-3)/2 - i) &= 1 \ , \\ \mathcal{M}_n(i, n-i-1) &= r_{2i}a_{2i} \ , \\ \mathcal{M}_n(i, n-i-2) &= r_{2i+1}a_{2i+1} \quad \text{for} \quad i = 0, \ldots, n-1 \ , \end{aligned}$$

where rows and columns of $\mathcal{M}_n(i, j)$ are numbered from 0 to $n-1$ and all elements of $\mathcal{M}_n$ are indexed modulo n.

Now permute the columns and rows of $\mathcal{M}_n$ in the following way. Decimate the rows as $i(n+1)/2$ and columns as $(n-3)/2 + i(n-1)/2$ modulo n for $i = 0, \ldots, n-1$ (note that $\gcd((n+1)/2, n) = \gcd((n-1)/2, n) = 1$). Then the obtained matrix $\mathcal{M}'_n$ is three-diagonal cyclic with

$$\begin{aligned} \mathcal{M}'_n(i, i) &= \mathcal{M}_n(i(n+1)/2, (n-3)/2 + i(n-1)/2) = 1 \ , \\ \mathcal{M}'_n(i, i-1) &= \mathcal{M}_n(i(n+1)/2, (n-3)/2 + (i-1)(n-1)/2) = r_{i(n+1)}a_{i(n+1)} \ , \\ \mathcal{M}'_n(i, i+1) &= \mathcal{M}_n(i(n+1)/2, (n-3)/2 + (i+1)(n-1)/2) = r_{i(n+1)+1}a_{i(n+1)+1} \end{aligned}$$

for $i = 0, \ldots, n-1$ (indices of r and a are calculated modulo $2n$) since

$$\begin{aligned} i(n+1)/2 + (n-3)/2 + i(n-1)/2 &= (n-3)/2 + in \equiv (n-3)/2 \pmod{n} \ , \\ i(n+1)/2 + (n-3)/2 + (i-1)(n-1)/2 &= -1 + in \equiv n-1 \pmod{n} \ , \\ i(n+1)/2 + (n-3)/2 + (i+1)(n-1)/2 &= n-2+in \equiv n-2 \pmod{n} \ . \end{aligned}$$

Also note that $a_{i(n+1)} = a_i$ since $a \in \mathrm{GF}(2^{nk})$ and $r_{i(n+1)} = r_i^{(-1)^i}$ since $r_{n+i} = r_n^{2^{ik}} = r_i^{-1}$ for any $i \geq 0$. Then for $i = 0, \ldots, n-1$

$$\mathcal{M}'_n(i, i+1) = r_{i+1}^{(-1)^i}a_{i+1} \quad \text{and} \quad \mathcal{M}'_n(i+1, i) = r_{i+1}^{(-1)^{i+1}}a_{i+1} \quad \text{so}$$

$$\mathcal{M}'_n = \begin{pmatrix} 1 & r_1a_1 & 0 & \cdots & r_0a_0 \\ r_1^{-1}a_1 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & & \ddots & 1 & r_{n-1}^{-1}a_{n-1} \\ r_0^{-1}a_0 & 0 & \cdots & r_{n-1}a_{n-1} & 1 \end{pmatrix} \ .$$

Note that a principal submatrix obtained by deleting the last column and the last row from $\mathcal{M}'_n$ is exactly $D_a^{1,n-2}$.

We also have to apply the decimation $(n-3)/2 + i(n-1)/2$ modulo n for $i = 0, \ldots, n-1$ (used to permute the columns of $\mathcal{M}$) to the vector of unknowns $(z_{2(n-1)}, z_{2(n-2)}, \ldots, z_2, z_0)$. This results in $\boldsymbol{z} = (z_{n+1}, z_2, z_{n+3}, \ldots, z_{n-1}, z_0)^{\mathrm{T}}$, where the increment for the index of z is equal to $n-1$ starting from 0 and going right to left (indices are calculated modulo $2n$). Now, if $\mathbf{0} = (0, \ldots, 0)^{\mathrm{T}}$ then a new system has the following matrix representation

$$\mathcal{M}'_n \boldsymbol{z} = \mathbf{0} \ . \tag{21}$$

The determinant of $\mathcal{M}_n$ is equal to the determinant of $\mathcal{M}'_n$ and can be computed expanding the latter by minors along the last row. Doing this it is easy to see that

$$\begin{aligned}
\det \mathcal{M}'_n \quad &= \quad \Delta'_a(1, n-2) + r_{n-1}a_{n-1}\left(r_{n-1}^{-1}a_{n-1}\Delta'_a(1, n-3) + \prod_{i=0}^{n-2} r_i^{(-1)^i} a_i\right) \\
&\qquad + r_0^{-1}a_0\left(r_0 a_0 \Delta'_a(2, n-2) + \prod_{i=1}^{n-1} r_i^{(-1)^{i-1}} a_i\right) \\
&\overset{(10,11,20)}{=} B_n^2(a) + a_{n-1}^2 B_{n-1}^2(a) + (a_0 B_{n-1}^{2^k}(a))^2 + \mathrm{N}_k^{nk}(a)(\delta + \delta^{-1}) \\
&\overset{(4,6)}{=} Z_n^2(a) + \mathrm{N}_k^{nk}(a)(\delta + \delta^{-1}) = Y_n(a) \ .
\end{aligned}$$

Thus, if $Y_n(a) \neq 0$ then (21) has only zero solution. Now note that every $v \in \mathrm{GF}(2^{2nk})$ with $L_a(v) = 0$ provides a solution to the system given by $v_{2i} = v^{2^{2ik}}$ for $i = 0, \ldots, n-1$. Therefore, if $Y_n(a) \neq 0$ then $L_a(z)$ has at most one zero.

Finally, note that if $Z_n(a) = 0$ (obviously, $a \neq 0$) then $Y_n(a) = \mathrm{N}_k^{nk}(a)(\delta + \delta^{-1}) \neq 0$ and thus, $L_a(z)$ has exactly one zero. □

Proposition 6 *For any $a \in \mathrm{GF}(2^{nk})^*$, $L_a(z)$ has at most 2^{2k} zeros in $\mathrm{GF}(2^{2nk})$.*

Proof. Consider the homogeneous system of linear equations (21) defined by matrix $\mathcal{M}'_n$ with $\boldsymbol{z} = (z_{n+1}, z_2, z_{n+3}, \ldots, z_{n-1}, z_0)^{\mathrm{T}}$. Note that a principal submatrix obtained by deleting the last column and the last row from $\mathcal{M}'_n$ is exactly $D_a^{1,n-2}$ and

$$\det D_a^{1,n-2} = \Delta'_a(1, n-2) \overset{(20)}{=} \Delta_a(1, n-2) \overset{(10)}{=} B_n^2(a) \ .$$

After removing the last equation from (21), we can write the remaining system as

$$D_a^{1,n-2}\boldsymbol{z}' = (r_0 a_0 z_0, 0, \ldots, 0, r_{n-1}^{-1}a_{n-1}z_0)^{\mathrm{T}} \ , \tag{22}$$

where $\boldsymbol{z}' = (z_{n+1}, z_2, z_{n+3}, \ldots, z_{n-1})^{\mathrm{T}}$ is obtained from $\boldsymbol{z}$ by deleting the last coordinate z_0.

Let $\widehat{D}_a^{1,n-2}$ denote the adjoint matrix of $D_a^{1,n-2}$ (it is well known that

$$D_a^{1,n-2}\widehat{D}_a^{1,n-2} = \widehat{D}_a^{1,n-2}D_a^{1,n-2} = \det D_a^{1,n-2} \cdot I_{n-1} = B_n^2(a) \cdot I_{n-1} \ ,$$

where I_{n-1} is the identity matrix of size $n-1$). Given a three-diagonal structure of $D_a^{1,n-2}$, it is easy to compute the elements of $\widehat{D}_a^{1,n-2}$ and to see that

$$\widehat{D}_a^{1,n-2}(1,0) = r_1^{-1}a_1 \det D_a^{3,n-2} \quad \text{and} \quad \widehat{D}_a^{1,n-2}(1,n-2) = r_2^{-1}a_2r_3a_3\cdots\cdots r_{n-2}a_{n-2} \ .$$

By (20), (10) and (11), $\det D_a^{3,n-2} = \Delta_a(3,n-2) = (B_{n-2}^2(a))^{2^{2k}}$. Also note that $\prod_{i=2}^{n-1} r_i^{(-1)^{i-1}} = r_0r_1^{-1}r^{-\frac{2^{nk}+1}{2^k+1}} = r_0r_1^{-1}\delta^{-1}$. Then, from (22) we get that

$$B_n^2(a)z_2 = r_0r_1^{-1}\left(a_0a_1(B_{n-2}^2(a))^{2^{2k}} + \delta^{-1}\prod_{i=2}^{n-1}a_i\right)z_0 \ . \tag{23}$$

Suppose that $L_a(z)$ has more than 2^{2k} zeros. These are also roots of equation (23) which has degree 2^{2k} and this is possible only if the latter equation is identically zero. Thus, in particular, $B_n(a) = 0$ and, by Lemma 2, $a = \frac{v_0^{2^{2k}+1}}{(v_0+v_1)^{2^k+1}}$ for some $v \in \mathrm{GF}(2^{nk}) \setminus \mathrm{GF}(2^k)$ with $\mathrm{Tr}_k^{nk}(v_0) = 0$. Also, necessarily,

$$\begin{aligned}
0 \ &= \ a_0a_1(B_{n-2}^2(a))^{2^{2k}} + \delta^{-1}\prod_{i=2}^{n-1}a_i \\
&\overset{(8)}{=} \frac{v_0v_1v_2v_3}{(v_0+v_1)(v_1+v_2)^2(v_2+v_3)}\left(\frac{\sum_{i=1}^{n-2}v_i\prod_{i=2}^{n-3}v_i}{\prod_{i=1}^{n-3}(v_i+v_{i+1})}\right)^{2^{2k+1}} \\
&\quad + \frac{\delta^{-1}\prod_{i=2}^{n-1}v_iv_{i+2}}{(v_2+v_3)\prod_{i=3}^{n-1}(v_i+v_{i+1})^2(v_n+v_{n+1})} \\
&= \ \frac{v_0v_1v_2v_3\sum_{i=3}^{n}v_i^2\prod_{i=4}^{n-1}v_i^2 + (v_1+v_2)^2\delta^{-1}\prod_{i=2}^{n-1}v_iv_{i+2}}{(v_0+v_1)(v_1+v_2)^2(v_2+v_3)\prod_{i=3}^{n-1}(v_i+v_{i+1})^2} \ .
\end{aligned}$$

Thus, since $\mathrm{Tr}_k^{nk}(v_0) = \sum_{i=0}^{n-1}v_i = 0$,

$$\begin{aligned}
0 &= v_0v_1v_2v_3\sum_{i=3}^{n}v_i^2\prod_{i=4}^{n-1}v_i^2 + (v_1+v_2)^2\delta^{-1}\prod_{i=2}^{n-1}v_iv_{i+2} \\
&= v_0v_1v_2v_3(v_1+v_2)^2\prod_{i=4}^{n-1}v_i^2 + (v_1+v_2)^2\delta^{-1}v_0v_1v_2v_3\prod_{i=4}^{n-1}v_i^2
\end{aligned}$$

which leads to $\delta = r^{\frac{2^{nk}+1}{2^k+1}} = 1$ which contradicts the condition imposed on r. $\square$

Proposition 7 *For any $a \in \mathrm{GF}(2^{nk})$, if $Y_n(a) = 0$ then $L_a(z)$ has 1 or 2^{2k} zeros in $\mathrm{GF}(2^{2nk})$. Moreover,*

$$\mathrm{Tr}_{2nk}(rav^{2^k+1}) + \mathrm{Tr}_{nk}(v^{2^{nk}+1}) = 0$$

for any $v \in \mathrm{GF}(2^{2nk})$ with $L_a(v) = 0$.

Proof. The first statement directly follows from Proposition 6. Let $V \neq 0$ be a zero of $L_a(z)$. Then all 2^{2k} zeros are given by μV for every $\mu \in \mathrm{GF}(2^{2k})$. For any $v \in \mathrm{GF}(2^{2nk})$ with $L_a(v) = 0$ we have $v = \mu V$ and

$$\begin{aligned}
\mathrm{Tr}_{2nk}\left(ra(\mu V)^{2^k+1}\right) + \mathrm{Tr}_{nk}\left((\mu V)^{2^{nk}+1}\right) &= \\
&= \mathrm{Tr}_{nk}\left(\mu^{2^k+1}(raV^{2^k+1} + r^{2^{nk}}a^{2^{nk}}V^{2^{(n+1)k}+2^{nk}} + V^{2^{nk}+1})\right) \\
&= \mathrm{Tr}_{k}\left(\mu^{2^k+1}\mathrm{Tr}_k^{nk}(raV^{2^k+1} + r^{-1}aV^{2^{(n+1)k}+2^{nk}} + V^{2^{nk}+1})\right) \\
&= \mathrm{Tr}_k(\mu^{2^k+1}Q) \ ,
\end{aligned}$$

where $Q = \mathrm{Tr}_k^{nk}(raV^{2^k+1} + r^{-1}aV^{2^{(n+1)k}+2^{nk}} + V^{2^{nk}+1})$. We show now that $Q = 0$. To this end, we define

$$U(a) = \sum_{y \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(ray^{2^k+1}) + \mathrm{Tr}_{nk}(y^{2^{nk}+1})}$$

and compute

$$\begin{aligned}
U^2(a) &= \sum_{x,y \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(ra(x^{2^k+1}+y^{2^k+1})) + \mathrm{Tr}_{nk}(x^{2^{nk}+1}+y^{2^{nk}+1})} \\
&= \sum_{y,v \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(ra((v+y)^{2^k+1}+y^{2^k+1})) + \mathrm{Tr}_{nk}((v+y)^{2^{nk}+1}+y^{2^{nk}+1})} \\
&= \sum_{y,v \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(ra(v^{2^k}y+vy^{2^k}+v^{2^k+1})+yv^{2^{nk}}) + \mathrm{Tr}_{nk}(v^{2^{nk}+1})} \\
&= \sum_{v \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(rav^{2^k+1}) + \mathrm{Tr}_{nk}(v^{2^{nk}+1})} \sum_{y \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(y^{2^k}L_a(v))} \\
&= 2^{2nk} \sum_{v \in \mathrm{GF}(2^{2nk}),\, L_a(v)=0} (-1)^{\mathrm{Tr}_{2nk}(rav^{2^k+1}) + \mathrm{Tr}_{nk}(v^{2^{nk}+1})} \\
&= 2^{2nk} \sum_{\mu \in \mathrm{GF}(2^{2k})} (-1)^{\mathrm{Tr}_k(\mu^{2^k+1}Q)} \ .
\end{aligned}$$

Suppose that $Q \neq 0$. When μ runs through $\mathrm{GF}(2^{2k})$ then $\mathrm{Tr}_k(\mu^{2^k+1}Q)$ takes on the value zero $M_0 = 1 + (2^k+1)(2^{k-1}-1)$ times and the value one $M_1 = (2^k+1)2^{k-1}$ times. Hence, $M_0 - M_1 = -2^k$ that implies

$$U(b)^2 = 2^{2nk}(M_0 - M_1) = -2^{(2n+1)k}$$

which is impossible. Thus, $Q = 0$ and the proposition is proved. □

5 Four-Valued Cross Correlation

In this section, we prove our main result formulated in Corollary 1. We start by considering the following exponential sum denoted $S_0(a)$ that to some extent is determined by the following lemma.

Lemma 3 *For an odd $n > 2$ and $a \in \mathrm{GF}(2^{nk})$ let $S_0(a)$ be defined by*

$$S_0(a) = \sum_{y \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(ay^{2^k+1}) + \mathrm{Tr}_{nk}(y^{2^{nk}+1})} \ .$$

Then

$$S_0(a) = 2^{nk} \sum_{v \in \mathrm{GF}(2^{nk}),\, A_a(v)=0} (-1)^{\mathrm{Tr}_{nk}(v)} \ ,$$

where $A_a(x)$ is defined in (3) with $c^{-1} = \delta + \delta^{-1}$ for δ being a primitive $(2^k+1)^{\text{th}}$ root of unity over $\mathrm{GF}(2)$.

Proof. Let δ be a primitive $(2^k+1)^{\text{th}}$ root of unity over $\mathrm{GF}(2)$ (note that $\delta \in \mathrm{GF}(2^{2k}) \setminus \mathrm{GF}(2^k)$). Then any element in $\mathrm{GF}(2^{2nk})$ can be written uniquely as $y = u + \delta v$ with $u, v \in \mathrm{GF}(2^{nk})$.

Let $\overline{y} = y^{2^{nk}}$ and $c^{-1} = \delta + \delta^{-1} \in \mathrm{GF}(2^k)$, then we obtain

$$\begin{aligned} y^{2^k+1} + \overline{y}^{2^k+1} &= (u+\delta v)^{2^k+1} + (u+\delta^{2^k} v)^{2^k+1} \\ &= (u^{2^k} v + u v^{2^k})(\delta + \delta^{2^k}) \\ &= c^{-1}(u^{2^k} v + u v^{2^k}) \end{aligned}$$

and further

$$\begin{aligned} y^{2^{nk}+1} &= (u+\delta v)^{2^{nk}+1} \\ &= u^{2^{nk}+1} + u^{2^{nk}} v\delta + u v^{2^{nk}} \delta^{2^{nk}} + v^{2^{nk}+1} \\ &= u^2 + c^{-1} uv + v^2 \ . \end{aligned}$$

Hence, we get

$$\begin{aligned}
S_0(a) &= \sum_{y\in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{nk}(a(y^{2^k+1}+\overline{y}^{2^k+1})+y^{2^{nk}+1})} \\
&= \sum_{u,v\in \mathrm{GF}(2^{nk})} (-1)^{\mathrm{Tr}_{nk}(ac^{-1}(u^{2^k}v+uv^{2^k})+u^2+c^{-1}uv+v^2)} \\
&= \sum_{v\in \mathrm{GF}(2^{nk})} (-1)^{\mathrm{Tr}_{nk}(v)} \sum_{u\in \mathrm{GF}(2^{nk})} (-1)^{\mathrm{Tr}_{nk}(u^{2^k}c^{-1}(a^{2^k}v^{2^{2k}}+v^{2^k}+av+c))} \\
&= 2^{nk} \sum_{v\in \mathrm{GF}(2^{nk}),\, A_a(v)=0} (-1)^{\mathrm{Tr}_{nk}(v)} \ ,
\end{aligned}$$

where $A_a(x) = a^{2^k}x^{2^{2k}} + x^{2^k} + ax + c$ and $c^{-1} = \delta + \delta^{-1}$. Consider equation $x^2 + c^{-1}x = 1$ that has two roots δ and δ^{-1} which are elements in $\mathrm{GF}(2^{2k})$ but not in $\mathrm{GF}(2^k)$. Letting $x = c^{-1}y$ we get $y^2 + y = c^2$ that has two solutions $c\delta$ and $c\delta^{-1}$ which do not belong to $\mathrm{GF}(2^k)$. Thus, $\mathrm{Tr}_k(c^2) = \mathrm{Tr}_k(c) = 1$. □

We can now determine $S_0(a)$ completely in the following corollary.

Corollary 4 *Under the conditions of Lemma 3 the distribution of $S_0(a)$ is given as follows:*

$$\begin{array}{rll}
-2^{nk} & \text{if} & Z_n(a) \neq 0 \ , \\
2^{(n+1)k} & \text{if} & Z_n(a) = 0 \text{ and } B_n(a) \neq 0 \ , \\
-2^{(n+2)k} & \text{if} & B_n(a) = 0 \ .
\end{array}$$

Proof. The distribution follows immediately from Lemma 3 and the results about the roots of $A_a(x)$ proved in Section 3. If $Z_n(a) \neq 0$ then we use Proposition 1, if $Z_n(a) = 0$ and $B_n(a) \neq 0$ then Proposition 2 comes in handy and, finally, if $B_n(a) = 0$ then we need Propositions 3 and 4. □

Lemma 4 *For an odd $n > 2$ and $a \in \mathrm{GF}(2^{nk})$ let $r = \alpha^{(2^{nk}-1)2^{k-1}}$, where α is a primitive element of $\mathrm{GF}(2^{2nk})$. Let also*

$$\begin{aligned}
S_j(a) &= \sum_{y\in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(r^j a y^{2^k+1})+\mathrm{Tr}_{nk}(y^{2^{nk}+1})} \quad \text{and} \\
S_{2^k+1-j}(a) &= \sum_{y\in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(r^{-j} a y^{2^k+1})+\mathrm{Tr}_{nk}(y^{2^{nk}+1})}
\end{aligned}$$

for $j = 1, 2, \ldots, 2^{k-1}$. Then

(i) $S_j(a) = S_{2^k+1-j}(a)$ for $j \in \{1, \ldots, 2^{k-1}\}$ and

(ii) $S_i(a)^2 = 2^{2nk} T_a$,

where T_a *is the number of zeros in* $\mathrm{GF}(2^{2nk})$ *of* $L_a(z)$ *defined in (19) with* r^i *(resp.* $r^{-(2^k+1-i)}$*) taken for* r *if* $1 \le i \le 2^{k-1}$ *(resp.* $2^{k-1} < i \le 2^k$*).*

Proof. (i) For any $j \in \{1, \ldots, 2^{k-1}\}$, straightforward calculations give

$$\begin{aligned} S_j(a) &= \sum_{y \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(r^{j2^{nk}} a^{2^{nk}} y^{(2^k+1)2^{nk}}) + \mathrm{Tr}_{nk}(y^{(2^{nk}+1)2^{nk}})} \\ &= \sum_{x \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(r^{-j} a x^{2^k+1}) + \mathrm{Tr}_{nk}(x^{2^{nk}+1})} \\ &= S_{2^k+1-j}(a) \ . \end{aligned}$$

(ii) For any $i \in \{1, \ldots, 2^k\}$ let $d(i) = i$ if $i \in \{1, \ldots, 2^{k-1}\}$ and $d(i) = -(2^k+1-i)$ if $i \in \{2^{k-1}+1, \ldots, 2^k\}$. Exactly the same way as in the calculations of $U^2(a)$ in Proposition 7 we obtain

$$\begin{aligned} S_i(a)^2 &= \sum_{x,y \in \mathrm{GF}(2^{2nk})} (-1)^{\mathrm{Tr}_{2nk}(r^{d(i)} a (x^{2^k+1} + y^{2^k+1})) + \mathrm{Tr}_{nk}(x^{2^{nk}+1} + y^{2^{nk}+1})} \\ &= 2^{2nk} \sum_{v \in \mathrm{GF}(2^{2nk}),\, L_a(v)=0} (-1)^{\mathrm{Tr}_{2nk}(r^{d(i)} a v^{2^k+1}) + \mathrm{Tr}_{nk}(v^{2^{nk}+1})} \ , \end{aligned}$$

where $L_a(z) = z^{2^{(n+1)k}} + r^{d(i)2^k} a^{2^k} z^{2^{2k}} + r^{d(i)} a z$. And, finally, we have

$$\mathrm{Tr}_{2nk}(r^{d(i)} a v^{2^k+1}) + \mathrm{Tr}_{nk}(v^{2^{nk}+1}) = 0$$

for any zero $v \in \mathrm{GF}(2^{2nk})$ of $L_a(z)$, by Propositions 5 and 7. □

We are now in position to completely determine the distribution of $S(a)$ defined in (2) for $a \in \mathrm{GF}(2^{nk})^*$. Since this is equivalent to the distribution of $C_d(\tau)+1$ for $\tau = 0, 1, \ldots, 2^{nk}-2$, our main result in Corollary 1 is a consequence of the theorem below.

Theorem 2 *Let* $m = 2nk$ *and* $d = \frac{2^{nk}+1}{2^k+1}$*, where* $n > 2$ *is odd and* $k > 1$*. Then the exponential sum* $S(a)$ *defined in (2) for* $a \in \mathrm{GF}(2^{nk})^*$ *(and* $C_d(\tau) + 1$*, for* $\tau = 0, 1, \ldots, 2^{nk} - 2$*) have the following distribution:*

$$\begin{array}{lll} -2^{(n+1)k} & \textit{occurs} & \frac{2^{(n-1)k}-1}{2^{2k}-1} \quad \textit{times} \ , \\ -2^{nk} & \textit{occurs} & \frac{(2^{nk}-1)(2^{k-1}-1)}{2^k-1} \quad \textit{times} \ , \\ 0 & \textit{occurs} & 2^{(n-1)k} - 1 \quad \textit{times} \ , \\ 2^{nk} & \textit{occurs} & \frac{(2^{nk}+1)2^{k-1}}{2^k+1} \quad \textit{times} \ . \end{array}$$

Proof. Take α being a primitive element of $\mathrm{GF}(2^{2nk})$ and let $\mathrm{ind}(x)$ be defined as $x = \alpha^{\mathrm{ind}(x)}$ for any $x \in \mathrm{GF}(2^{2nk})$. Letting also $r = \alpha^{(2^{nk}-1)2^{k-1}}$ we observe that $r^{2^{nk}+1} = 1$ and that r^i is not a $(2^k+1)^{\text{th}}$ power in $\mathrm{GF}(2^{2nk})$ for any $i = 1, 2, \ldots, 2^{k-1}$ since $\mathrm{ind}(r^i) \equiv i \pmod{2^k+1}$. It is also clear that $\mathrm{ind}(r^{-i}) \equiv 2^{2nk} - 1 - \mathrm{ind}(r^i) \equiv 2^k + 1 - i \pmod{2^k+1}$.

Finding the distribution of the cross-correlation function $C_d(\tau) + 1$ is equivalent to computing the distribution of $S(a)$ defined in (2) for $a \in \mathrm{GF}(2^k)^*$. To calculate $S(a)$, we first observe that $\gcd(2^k+1, 2^m-1) = 2^k+1$. If we first let $x = y^{2^k+1}$ then $x = r^i y^{2^k+1}$ and, finally, $x = r^{-i} y^{2^k+1}$ for $i = 1, \ldots, 2^{k-1}$ and y running through $\mathrm{GF}(2^m)$ then x will run through $\mathrm{GF}(2^m)$ in total 2^k+1 times. Further, since $d(2^k+1)(2^{nk}+1) \equiv 2(2^{nk}+1) \pmod{2^m-1}$, we obtain

$$\begin{aligned}(2^k+1)S(a) = &\sum_{i=0}^{2^{k-1}} \sum_{y \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(r^i a y^{2^k+1}) + \mathrm{Tr}_{nk}(y^{2^{nk}+1})} \\ &+ \sum_{i=1}^{2^{k-1}} \sum_{y \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(r^{-i} a y^{2^k+1}) + \mathrm{Tr}_{nk}(y^{2^{nk}+1})} = \sum_{i=0}^{2^k} S_i(a) \ ,\end{aligned}$$

where $S_i(a)$ are defined as in Lemma 4. We divide the proof into three cases.

Case 1: $(B_n(a) = 0)$

In this case, Corollary 4 gives $S_0(a) = -2^{(n+2)k}$ and, by Proposition 5, $L_a(z)$ has exactly one zero (since $Z_n(a) = 0$ by (12)). Therefore, by Lemma 4 (ii), $S_i(a) = \pm 2^{nk}$ for all values of $i = 1, 2, \ldots, 2^k$. Thus,

$$(2^k+1)S(a) = -2^{(n+2)k} + t2^{nk} \ ,$$

where $|t| \le 2^k$. Reduce both sides of the latter identity modulo 2^k+1 to obtain $1 - t \equiv 0 \pmod{2^k+1}$. Since t is even then $t \neq 1$ and the only possibility is $t = -2^k$ leading to $S(a) = -2^{(n+1)k}$.

Case 2: $(Z_n(a) = 0$ and $B_n(a) \neq 0)$

In this case, Corollary 4 gives $S_0(a) = 2^{(n+1)k}$ and, by Proposition 5, $L_a(z)$ has exactly one zero. Therefore, by Lemma 4 (ii), $S_i(a) = \pm 2^{nk}$ for all values of $i = 1, 2, \ldots, 2^k$. Thus,

$$(2^k+1)S(a) = 2^{(n+1)k} + t2^{nk} \ ,$$

where $|t| \le 2^k$. Reduce both sides of the latter identity modulo 2^k+1 to obtain $1 - t \equiv 0 \pmod{2^k+1}$. Since t is even then $t \neq 1$ and the only possibility is $t = -2^k$ leading to $S(a) = 0$.

Case 3: $(Z_n(a) \neq 0)$

In this case, Corollary 4 gives $S_0(a) = -2^{nk}$. Consider a set of 2^{k-1} values

$$Y_n(a) = Z_n^2(a) + \mathrm{N}_k^{nk}(a)(\delta^j + \delta^{-j}) \quad \text{for} \quad j = 1, 2, \ldots, 2^{k-1} \ ,$$

where $\delta = \alpha^{\frac{(2^{2nk}-1)2^{k-1}}{2^k+1}}$ is an element of multiplicative order 2^k+1. If quadratic equation $x + x^{-1} = Z_n^2(a)/\mathrm{N}_k^{nk}(a)$ has two solutions then the product of these is one and thus, there is at most one zero (say, when $j = \mathcal{J}$) in this set. Therefore, by Propositions 5, 7 and Lemma 4 (ii), $S_i(a) = \pm 2^{nk}$ for all values of $i = 1, 2, \ldots, 2^k$ except for, possibly, two with $i = \mathcal{J}$ and $i = 2^k + 1 - \mathcal{J}$ when $S_{\mathcal{J}}(a) = S_{2^k+1-\mathcal{J}}(a) = \pm 2^{(n+1)k}$, using Lemma 4 (i).

In the case when $S_i(a) = \pm 2^{nk}$ for all values of $i = 1, 2, \ldots, 2^k$, we have

$$(2^k + 1)S(a) = -2^{nk} + t2^{nk} \ ,$$

where $|t| \le 2^k$. Reduce both sides of the latter identity modulo $2^k + 1$ to obtain $1 - t \equiv 0 \pmod{2^k + 1}$. Since t is even then $t \ne 1$ and the only possibility is $t = -2^k$ leading to $S(a) = -2^{nk}$.

Finally, in the case when $S_i(a) = \pm 2^{nk}$ for all values of $i = 1, 2, \ldots, 2^k$ except for two, we have

$$(2^k + 1)S(a) = -2^{nk} + t2^{nk} + \varepsilon 2^{(n+1)k+1} \ ,$$

where $|t| \le 2^k - 2$ and $\varepsilon \in \{-1, +1\}$. Reduce both sides of the latter identity modulo $2^k + 1$ to obtain $1 - t + 2\varepsilon \equiv 0 \pmod{2^k + 1}$. Since t is even then $t \notin \{-1, 3\}$ and the only possibility is $t = -(2^k - 2)$ and $\varepsilon = 1$ leading to $S(a) = 2^{nk}$.

The three cases above give, in total, the possible values 0, $\pm 2^{nk}$ and $-2^{(n+1)k}$ for $S(a)$. Suppose the cross-correlation function $C_d(\tau)+1$ takes on the value zero r times, the value 2^{nk} is taken on s times, the value -2^{nk} occurs t times and the value $-2^{(n+1)k}$ occurs v times. Since $S(a) = -2^{(n+1)k}$ is possible only in Case 1, when $B_n(a) = 0$, then, by Lemma 2, $v = \frac{2^{(n-1)k}-1}{2^{2k}-1}$. By Proposition 2, the number of $a \in \mathrm{GF}(2^{nk})^*$ such that $Z_n(a) = 0$ and $B_n(a) \ne 0$ is equal $2^{(n-1)k} - 1$. Thus, since $S(a) = 0$ is possible only in Case 2, when $Z_n(a) = 0$ and $B_n(a) \ne 0$, then $r = 2^{(n-1)k} - 1$.

For the remaining values of $S(a) = \pm 2^{nk}$, obviously,

$$s + t = 2^{nk} - 1 - (r + v) = \frac{2^{(n+2)k} - 2^{(n+1)k} - 2^{nk} + 1}{2^{2k} - 1} \ .$$

On the other hand, from Lemma 1 it follows that

$$2^{nk}s - 2^{nk}t - 2^{(n+1)k}v = 2^{nk}(s - t) - \frac{2^{(n+1)k}(2^{(n-1)k} - 1)}{2^{2k} - 1} = 2^{nk}$$

and

$$s - t = 1 + \frac{2^k(2^{(n-1)k} - 1)}{2^{2k} - 1} = \frac{2^{nk} + 2^{2k} - 2^k - 1}{2^{2k} - 1} \ .$$

Thus, the solutions are $s = \frac{(2^{nk}+1)2^{k-1}}{2^k+1}$ and $t = \frac{(2^{nk}-1)(2^{k-1}-1)}{2^k-1}$. □

The arguments in this paper also work for $k = 1$. However, in this case, the corresponding decimation $d = (2^n + 1)/3$ is only three-valued (see [4]). Indeed, in this case,

$$3S(a) = S_0(a) + S_1(a) + S_2(a) = S_0(a) + 2S_1(a) \ .$$

It was proved in Proposition 1 that $Z_n(a) \in \mathrm{GF}(2^k) = \mathrm{GF}(2)$. Thus, if $Z_n(a) \neq 0$ then $Z_n(a) = 1$ and the value of $S_1(a)$ is defined by whether

$$Y_n(a) = Z_n^2(a) + \mathrm{N}_1^n(a)(\delta + \delta^{-1}) = 1 + \delta + \delta^{-1} \ ,$$

where $\delta = \alpha^{(2^{2n}-1)/3}$ is primitive in $\mathrm{GF}(4)$, is zero or not (note that $a \neq 0$). Since $\delta + 1 = \delta^2 = \delta^{-1}$, we have $\delta + \delta^{-1} = 1$. Therefore, if $Z_n(a) \neq 0$ then $S(a) = 2^n$ and is never equal to -2^n. This reduces the four-valued cross-correlation case to three values.

6 Conclusions

We have identified new pairs of m-sequences having different lengths $2^{2nk} - 1$ and $2^{2k} - 1$, where $n > 2$ is odd and $k > 1$, with four-valued cross correlation and we have completely determined the cross-correlation distribution. These pairs differ from the sequences in the Kasami family by the property that instead of the decimation $d = 1$ we take $d = \frac{2^{nk}+1}{2^k+1}$.

References

[1] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Mathematics*, vol. 16, no. 3, pp. 209–232, Nov. 1976.

[2] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook in Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier Science B.V., 1998, vol. II, ch. 21, pp. 1765–1853.

[3] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 613–627, Feb. 2006.

[4] G. J. Ness and T. Helleseth, "Cross correlation of m-sequences of different lengths," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1637–1648, Apr. 2006.

[5] T. Kasami, "Weight distribution formula for some classes of cyclic codes," Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285 (AD 637524), Apr. 1966.

[6] G. J. Ness and T. Helleseth, "A new three-valued cross correlation between m-sequences of different lengths," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4695–4701, Oct. 2006.

[7] T. Helleseth, A. Kholosha, and G. J. Ness, "Characterization of m-sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued crosscorrelation," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2236–2245, Jun. 2007.

[8] G. J. Ness and T. Helleseth, "A new family of four-valued cross correlation between m-sequences of different lengths," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4308–4313, Nov. 2007.

[9] V. P. Il'in and Y. I. Kuznetsov, *Three-Diagonal Matrices and their Applications*. Moscow: Nauka, 1985, (in Russian).

[10] A. W. Bluher, "On $x^{q+1} + ax + b$," *Finite Fields and Their Applications*, vol. 10, no. 3, pp. 285–305, Jul. 2004.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, ser. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 1997, vol. 20.